On the Asymptotic Performance of Iterative Decoders for Product Codes

Moshe Schwartz
University of California San Diego
9500 Gilman Drive, Mail Code 0407
La Jolla, CA 92093-0407, U.S.A.
moosh@everest.ucsd.edu

Paul H. Siegel
University of California San Diego
9500 Gilman Drive, Mail Code 0401
La Jolla, CA 92093-0401, U.S.A.
psiegel@ucsd.edu

Alexander Vardy
University of California San Diego
9500 Gilman Drive, Mail Code 0407
La Jolla, CA 92093-0407, U.S.A.
vardy@kilimanjaro.ucsd.edu

***Abstract*— We consider hard-decision iterative decoders for product codes over the erasure channel, which employ repeated rounds of decoding rows and columns alternatingly. We derive the exact asymptotic probability of decoding failure as a function of the error-correction capabilities of the row and column codes, the number of decoding rounds, and the channel erasure probability. We examine both the case of codes capable of correcting a constant amount of errors, and the case of codes capable of correcting a constant fraction of their length.**

I. Introduction

One of the simplest methods of combining two codes is the product construction. Let C_1 and C_2 be $[n_1, k_1, d_1]$ and $[n_2, k_2, d_2]$ linear codes respectively. Then, the set of $n_1 \times n_2$ arrays whose columns are codewords of C_1 and whose rows are codewords of C_2, is the product code $C_1 \otimes C_2$ with parameters $[n_1 n_2, k_1 k_2, d_1 d_2]$.

Product codes are useful in a variety of applications (for references see [1]). They may be found in the ubiquitous CD standard IEC-908 and CD-ROM standard ECMA-130 (for details see [2]), as well as the DVD standard (`www.dvdforum.org`). Their rectangular shape makes them especially appealing to two-dimensional error-control applications (for references see [3]).

The fact that product codes retain entire codewords of their constituent codes makes it tempting to use an iterative decoder in the following fashion. First, each of the columns is decoded using a decoder for C_1. The resulting (partially) decoded array is then used for a new round of decoding in which each row is decoded using a decoder for C_2. This process may be carried for any number of rounds deemed necessary, alternatingly decoding rows and columns. It is therefore a natural question to ask what is the decoding-failure probability of such a scheme.

This probability is obviously a function of the amount of errors correctable by the columns and row codes, the number of decoding rounds, and the channel error probability. The channel need not be binary, and we assume that it introduces an error in a certain position independently of other positions, and with the same distribution. We use the row and column decoders as black boxes with the only assumption being that they do not misdecode, i.e., they either correct all the errors or do nothing. This is the case when we take the q-ary erasure channel.

In this work we calculate the asymptotic decoding-failure probability. This is a rare case where we can precisely predict the performance of iterative decoding analytically for a specific code rather than a random ensemble. We manage this by recasting the problem to a graph-theoretic setting in which the channel is thought of as producing random bi-partite graphs. By doing so, we can rely on well-known mechanisms for checking properties of random graphs.

The paper is organized as follows. In Section II we give some necessary background on random graphs. We continue to Section III, in which we examine row and column codes which can correct a constant number of errors. This will be referred to as the *constant error correction case*. In Section IV we handle the case of row and column codes capable of correcting a constant fraction of their length, which we will call the *linear error correction case*. We conclude in Section V with a discussion of the results.

II. Background

Let us examine the case where we have a product code with codewords of size $n \times n$, and the column code and row codes are each capable of correcting t errors. After passing through the channel, a received word may contain errors. We can represent these errors as a bi-partite graph $G = (V_L, V_R, E)$ with a vertex in $V_L = \{1, \ldots, n\}$ for each row, and a vertex in $V_R = \{n+1, \ldots, 2n\}$ for each column. An edge (i, j) is in E if and only if position $(i, j-n)$ is in error.

Let n_L and n_R be positive integers, and let $0 \leq p \leq 1$. The *random bi-partite graph*, $G(n_L, n_R, p)$, is a probability space over the set of bi-partite graphs on the vertex set $V = V_L \cup V_R$, where $|V_L| = n_L$, $|V_R| = n_R$, $V_L \cap V_R = \emptyset$, and with

$$\Pr[(i,j) \in G] = \begin{cases} p & i \in V_L, j \in V_R \\ 0 & \text{otherwise,} \end{cases}$$

with these mutually independent. Hence, we can think of our channel as producing a random bi-partite graph $G(n, n, p)$.

A *round* of decoding consists of an attempt to decode either all the rows, or all the columns. When viewed in the bi-partite graph representation, a decoding round consists of going over either the vertices of V_L or the vertices of V_R, and for each

vertex with degree less or equal to t, removing all of its adjacent edges. Successive rounds alternate between rows and columns. We assume, w.l.o.g., that the last round is always performed on the rows. We denote the number of rounds as r, where r is a constant.

Given a bi-partite graph, G, representing the transmission errors, we say that it is (r,t)-*decodable* if a decoder which can correct up to t errors in each row and column, corrects all the errors after r rounds. In other words, after r rounds of edge removals as described above, no edges remain. Our aim is to analyze the asymptotic probability of decoding failure.

Throughout this paper we follow the notation of [4]. Given two functions, $f(n)$ and $g(n)$, we say that $f(n) \ll g(n)$ if $f(n) = o(g(n))$. Let G be a graph, and let A be a graph-theoretic property. If G has property A, we denote it by $G \models A$. In our case, A is the property that the graph is (r,t)-decodable. As mentioned in [4], many graph-theoretic properties exhibit a threshold behavior as follows.

Definition 1: $r(n)$ is called a threshold function for a graph theoretic property A if

- When $p(n) \ll r(n)$, $\lim_{n\to\infty} \Pr[G(n,n,p(n)) \models A] = 0$.
- When $p(n) \gg r(n)$, $\lim_{n\to\infty} \Pr[G(n,n,p(n)) \models A] = 1$.

Finally, given some event A whose probability depends on some parameter n, we say that A occurs *almost always* if $\lim_{n\to\infty} \Pr[A] = 1$.

III. The Constant Error Correction Case

In this section we handle the case where both the column and row codes are capable of correcting a constant t number of errors. This is done by first noting that a bi-partite graph representing the transmission errors is decodable if and only if it does not contain a certain subgraph which we call an (r,t)-*undecodable configuration*. We then continue, using the theory of random graphs, to analyze the probability that the random bi-partite graph contains this undecodable configuration. We need the following definitions first.

Definition 2: Let $G = (V,E)$ be a graph, and let $v \in V$ be a vertex of the graph. We denote by $N_i(v)$ the set of vertices of G which are reachable from v by a path (not necessarily simple) of length exactly i.

We note that under this definition, a vertex of degree at least 1 is its own neighbor at distance 2, since we can take a path going over an outgoing edge, and returning by the same edge. In fact, such a vertex is its own neighbor for any even distance. We denote the degree of vertex $v \in V$ as $d(v)$.

Definition 3: Let $G = (V_L, V_R, E)$ be a bi-partite graph. We say that G is an (r,t)-*undecodable configuration* if there exists $v \in V_L$ such that all the following hold:

- $\bigcup_{i=0}^{r} N_i(v) = V_L \cup V_R$.
- For all $0 \le i \le r-1$ and $v' \in N_i(v)$, $d(v') \ge t+1$.

We call v the *root* of G.

Note that by the first requirement, the graph must be connected. Hence, the sets $N_i(v)$ are not disjoint, and both

$$N_0(v) \subseteq N_2(v) \subseteq N_4(v) \subseteq \dots$$

and

$$N_1(v) \subseteq N_3(v) \subseteq N_5(v) \subseteq \dots$$

hold. Furthermore, if $v' \in N_i(v)$ for some $i \ge 0$, then its immediate neighbors are all in $N_{i+1}(v)$.

Definition 4: Let $G = (V_L, V_R, E)$ be a bi-partite graph, and let $H = (V'_L, V'_R, E')$ be another bi-partite graph. We say that H is an *ordered bi-partite subgraph* of G if there exist injective functions $f_L : V'_L \to V_L$ and $f_R : V'_R \to V_R$ such that if $(v_1, v_2) \in E'$, then $(f_L(v_1), f_R(v_2)) \in E$.

The following theorem is the basis for our analysis.

Theorem 1: A bi-partite graph $G = (V_L, V_R, E)$ is (r,t)-decodable if and only if it does not have an (r,t)-undecodable configuration as an ordered bi-partite subgraph.

Proof: In the first direction, let us assume that G contains an (r,t)-undecodable graph H as an ordered bi-partite subgraph. Let v be the root of H. In the first round of decoding G, the vertices corresponding to $N_{r-1}(v)$ are not decoded since they have degree of at least $t+1$. In the following round, if we take any vertex $v' \in N_{r-2}(v)$, all of its neighbors are in $N_{r-1}(v)$ so they were not corrected in the first round. Since v' has degree at least $t+1$, it follows that the vertices of $N_{r-2}(v)$ are not corrected in the second round. Continuing in the same manner, after r rounds, the sole vertex of $N_0(v) = \{v\}$ is not corrected, so G is not (r,t)-decodable.

In the other direction, let G be a graph which is not (r,t)-decodable. Hence, after r rounds of decoding, there exists a vertex $v \in V_L$ which was not corrected. We now show that v is the root of an (r,t)-undecodable configuration $H = (V'_L, V'_R, E')$ which is an ordered bi-partite subgraph of G. We start by obviously defining $N_0(v) = \{v\}$ and taking $V'_L = \{v\}$, $V'_R = \emptyset$, and $E' = \emptyset$. Now, since v was not decoded at the end of round r, round $r-1$ ended with v having at least $t+1$ undecoded neighbors. We denote this set of neighbors as $N_1(v)$. We also add these neighbors to V'_R and the appropriate edges to E'. Take some $v' \in N_1(v)$. Since v' was not decoded at the end of round $r-1$, round $r-2$ ended with v' having at least $t+1$ undecoded neighbors. Going over all possible $v' \in V'_R$, and taking the union of the undecoded neighbors we get $N_2(v)$. Note that $N_0(v) \subseteq N_2(v)$. We add $N_2(v)$ to V'_L and the appropriate edges to E'. Continuing in the same manner we get an (r,t)-undecodable configuration as the theorem states. ∎

By the previous theorem, the question of undecodability becomes a purely graph-theoretic question. For the asymptotic analysis we need the following definitions and probabilistic tools.

Theorem 2 ([4]): Let X be a non-negative integral-valued random variable. If $E[X] = o(1)$, then $X = 0$ almost always.

Proof: Trivial. ∎

For the rest of this section, let $X = X_1 + \dots + X_m$ where X_i is the indicator random variable for event A_i. For indices i, j, we write $i \sim j$ if $i \ne j$ and events A_i and A_j are not independent. We define

$$\Delta = \sum_{i\sim j} \Pr[A_i \wedge A_j].$$

Theorem 3 (Corollary 4.3.4, [4]): If $E[X] \to \infty$ and $\Delta = o(E[X]^2)$, then $X > 0$ almost always.

Definition 5 ([4]): Let H be a graph with v vertices and e edges. We call $\rho = e/v$ the *density* of H. We call H *balanced* if every subgraph H' has $\rho(H') \leq \rho(H)$. We call H *strictly balanced* if every proper subgraph H' has $\rho(H') < \rho(H)$.

The following is an adaptation of Theorem 4.4.2, [4], to bi-partite random graphs.

Theorem 4: Let H be a balanced bi-partite graph with v vertices and e edges. Let $G(n, n, p)$ be a random bi-partite graph, and let A be the event that H is an ordered bi-partite subgraph of G. Then $p = n^{-v/e}$ is the threshold function for A.

Proof: Let $H = (V'_L, V'_R, E')$ be a balanced bi-partite graph. Denote $v_L = |V'_L|$, and $v_R = |V'_R|$, so $v = v_L + v_R$. Let $G = (V_L, V_R, E)$ be a random bi-partite graph. Let S be a v-subset of the vertices of G such that $|S \cap V_L| = v_L$ and $|S \cap V_R| = v_R$. Let A_S be the event that the subgraph of G induced by S contains H as an ordered bi-partite subgraph. Then obviously,

$$p^e \leq \Pr[A_S] \leq v_L! v_R! p^e.$$

Let X_S be the indicator random variable for A_S and

$$X = \sum_S X_S.$$

By linearity of expectation,

$$E[X] = \sum_S E[X_S] = \binom{n}{v_L}\binom{n}{v_R} \Pr[A_S] = \Theta(n^v p^e).$$

If $p(n) \ll n^{-v/e}$ then $E[X] = o(1)$, so by Theorem 2, $X = 0$ almost always.

Now assume $p(n) \gg n^{-v/e}$ so that $E[X] \to \infty$, and consider Δ of Theorem 3.

$$\Delta = \sum_{S \sim T} \Pr[A_S \wedge A_T] = \sum_S \Pr[A_S] \sum_{T \sim S} \Pr[A_T | A_S].$$

Here, two v-sets S and T satisfy $S \sim T$ if and only if $S \neq T$ and they share some edges, i.e., $|S \cap T \cap V_L| \geq 1$ and $|S \cap T \cap V_R| \geq 1$. Let S be fixed, so

$$\sum_{T \sim S} \Pr[A_T | A_S] = \sum_{i=2}^{v-1} \sum_{\substack{|S \cap T| = i \\ |S \cap T \cap V_L| \geq 1 \\ |S \cap T \cap V_R| \geq 1}} \Pr[A_T | A_S].$$

For each i there are $O(n^{v-i})$ choices of T. Fix S and T, and consider $\Pr[A_T|A_S]$. There are $O(1)$ possible copies of H on T. Since H is balanced, each has at most $\frac{ie}{v}$ edges with both vertices in S, hence at least $e - \frac{ie}{v}$ other edges. Therefore,

$$\Pr[A_T | A_S] = O(p^{e - \frac{ie}{v}}),$$

and

$$\begin{aligned}\sum_{T \sim S} \Pr[A_T | A_S] &= \sum_{i=2}^{v-1} O(n^{v-i} p^{e - \frac{ie}{v}}) \\ &= \sum_{i=2}^{v-1} O((n^v p^e)^{1 - \frac{i}{v}}) = \sum_{i=2}^{v-1} o(n^v p^e) = o(E[X]),\end{aligned}$$

since $p(n) \gg n^{-v/e}$. We have already seen that $\Pr[A_S] = O(p^e)$, and there are $O(n^v)$ choices for S, so

$$\begin{aligned}\Delta &= \sum_S \Pr[A_S] \sum_{T \sim S} \Pr[A_T | A_S] \\ &= O(n^v p^e) o(E[X]) = o(E[X]^2).\end{aligned}$$

By Theorem 3, $X > 0$ almost always. ∎

Let us start by examining one specific type of an (r, t)-undecodable configuration. We define an *exact* (r, t)-*undecodable tree* as an (r, t)-undecodable configuration without cycles in which each vertex at distance at most $r - 1$ from the root has degree $t + 1$ exactly. It is easy to see that such a graph is strictly balanced. We denote the number of edges in such a tree as $e_T(r, t)$. This number is easily seen to be:

$$e_T(r, t) = \begin{cases} 2r & t = 1 \\ (t+1)\frac{t^r - 1}{t - 1} & t \geq 2. \end{cases} \tag{1}$$

Since this is a tree, obviously the number of vertices $v_T(r, t)$ is exactly $e_T(r, t) + 1$. By Theorem 4, the threshold function for the existence of an exact (r, t)-undecodable tree in $G(n, n, p)$ is

$$p = n^{-\left(1 + \frac{1}{e_T(r,t)}\right)}. \tag{2}$$

Another case is when the (r, t)-undecodable tree is not exact, i.e., the configuration is a tree, but some vertices at distance at most $r - 1$ from the root have a degree which is strictly more than $t+1$. However, in such a case, the existence of a non-exact (r, t)-undecodable tree implies the existence of an exact (r, t)-undecodable tree (simply trim the excess edges and vertices).

Thus we are left with the case of (r, t)-undecodable configurations which are not trees at all. Such configurations must contain cycles. It is also easy to see that such configurations must contain a simple cycle with at most $2r$ edges.

If we take a graph of a simple cycle with e edges, it also has e vertices. This graph is also strictly balanced. It follows that the threshold function for the existence of such a cycle is $p = n^{-1}$. Hence, when (2) holds, or when

$$p \ll n^{-\left(1 + \frac{1}{e_T(r,t)}\right)},$$

there are almost always no simple cycles of length at most $2r$. This is because each length almost always does not appear, and there are $O(1)$ such lengths which interest us, so a simple union bound suffices. Thus, there are almost always no (r, t)-undecodable configurations with cycles in $G(n, n, p)$ under these conditions.

Corollary 1: The threshold function for the existence of an (r,t)-undecodable configuration in $G(n,n,p)$, for some fixed r and t, is

$$p = n^{-\left(1+\frac{1}{e_T(r,t)}\right)},$$

where $e_T(r,t)$ is given by (1).

Now that we have established a threshold behavior for the existence of (r,t)-undecodable configurations, we are left with the case where

$$p = c \cdot n^{-\left(1+\frac{1}{e_T(r,t)}\right)},$$

for some constant $c > 0$. We know that in this case, the question of the existence of an (r,t)-undecodable configuration in $G(n,n,p)$ reduces to the question of the existence of an exact (r,t)-tree in $G(n,n,p)$.

For the following analysis we need the Janson inequality [5]. Let Ω be a finite universal set, and let R be a random subset of Ω given by

$$\Pr[r \in R] = p_r,$$

where these events are mutually independent. Let B_i, $i \in I$ be subsets of Ω, where I is a finite index set. Let A_i be the event that $B_i \subseteq R$. Let X_i be the indicator variable for A_i, and let $X = \sum_{i \in I} X_i$. We denote the complementary event to A_i as $\overline{A_i}$. We set

$$M = \prod_{i \in I} \Pr[\overline{A_i}].$$

Theorem 5 (The Janson Inequality, [5]): Let A_i, $i \in I$, Δ, and M, be as above, and assume that $\Pr[A_i] \leq \epsilon$ for all $i \in I$. Then

$$M \leq \Pr[\wedge_{i \in I} \overline{A_i}] \leq M e^{\frac{1}{1-\epsilon}\frac{\Delta}{2}}.$$

We can now continue by adapting Theorem 10.1.1, [4], to bi-partite graphs.

Theorem 6: Let H be a strictly-balanced bi-partite graph with v vertices, e edges, and a automorphisms. Let $c > 0$ be some constant. We denote by A the event that G does not have H as an ordered bi-partite subgraph. Then, when $p = c \cdot n^{-v/e}$ we have,

$$\lim_{n \to \infty} \Pr[G(n,n,p) \models A] = exp[-c^e/a].$$

Proof: Let $H = (V'_L, V'_R, E')$ be a strictly-balanced bi-partite graph. Denote $v_L = |V'_L|$, and $v_R = |V'_R|$, so $v = v_L + v_R$. Let B_i, $1 \leq i \leq \binom{n}{v_L}\binom{n}{v_R} v_L! v_R!/a$, range over the edge sets of possible placements of H as an ordered bi-partite subgraph of G. Let A_i be the event that $B_i \subseteq G(n,n,p)$.

We use Janson's inequality from Theorem 5. For all i, $\Pr[A_i] = p^e$, so

$$\lim_{n \to \infty} M = \lim_{n \to \infty} (1-p^e)^{\binom{n}{v_L}\binom{n}{v_R} v_L! v_R!/a} = exp[-c^e/a],$$

since $p = c \cdot n^{-v/e}$. We turn to handle

$$\Delta = \sum_{i \sim j} \Pr[A_i \wedge A_j].$$

When $i \sim j$, let k denote the number of vertices in the intersection of the two placements of H. Obviously $2 \leq k \leq v$. Let f_k denote the maximal number of edges in the intersection when $i \sim j$ and there are k vertices in the intersection. For $k = v$ we obviously have $f_v < e$ since $i \neq j$. When $2 \leq k \leq v-1$, since H is strictly-balanced and $B_i \cap B_j$ is a subgraph of H,

$$\frac{f_k}{k} < \frac{e}{v}.$$

There are $O(n^{2v-k})$ choices of i and j which intersect in k vertices. Hence, for each such i and j,

$$\Pr[A_i \wedge A_j] = p^{|B_i \cup B_j|} = p^{2e-|B_i \cap B_j|} \leq p^{2e-f_k},$$

and then

$$\Delta = \sum_{k=2}^{v} O(n^{2v-k}) O(n^{-\frac{v}{e}(2e-f_k)}).$$

But

$$2v - k - \frac{v}{e}(2e - f_k) = \frac{v f_k}{e} - k < 0,$$

so $\Delta = o(1)$. Janson's inequalities become a sandwich, so

$$\lim_{n \to \infty} \Pr[\wedge_i \overline{A_i}] = \lim_{n \to \infty} M = exp[-c^e/a].$$

■

Fortunately, an exact (r,t)-tree is strictly balanced, and has the following number of automorphisms:

$$a_T(r,t) = \begin{cases} 2 & t = 1 \\ (t+1)!(t!)^{(t+1)\frac{t^{r-1}-1}{t-1}} & t \geq 2. \end{cases} \quad (3)$$

Thus we get the following corollary:

Corollary 2: The probability that $G(n,n,p)$ is (r,t)-decodable when $p = c \cdot n^{-\left(1+\frac{1}{e_T(r,t)}\right)}$, is asymptotically $exp[-c^{e_T(r,t)}/a_T(r,t)]$, where $e_T(r,t)$ is given by (1) and $a_T(r,t)$ is given by (3).

Finally, we summarize the case of constant error correction in Table I.

TABLE I

THE ASYMPTOTIC PROBABILITY OF DECODER FAILURE WITH r ROUNDS OF DECODING, A CONSTANT t OF DECODABLE ERRORS IN EACH ROW AND COLUMN, AND ERASURE PROBABILITY p

$p(n)$	Decodability
$p \ll n^{-\left(1+\frac{1}{e_T(r,t)}\right)}$	Almost always decodable
$p = c \cdot n^{-\left(1+\frac{1}{e_T(r,t)}\right)}$	Decodable with probability $exp[-c^{e_T(r,t)}/a_T(r,t)]$
$p \gg n^{-\left(1+\frac{1}{e_T(r,t)}\right)}$	Almost always undecodable

IV. THE LINEAR ERROR CORRECTION CASE

We now turn to the case of linear error correction capabilities. This case appears to be much simpler than the previous one. Let $F = \{C_1, C_2, \dots\}$ be an infinite family of codes of ever increasing length, and let us denote the length of C_i by n_i. We now require that C_i is capable of correcting αn_i errors,

where $0 < \alpha < 1$ is some constant. We note that "good" codes also fall into this category.

Just like before, in this section we consider a product code having codewords of size $n \times n$. For convenience, the row code and the column code are each capable of correcting αn errors, where $0 < \alpha < 1$ is a constant. We denote by p the erasure probability of the channel.

The main tool for our analysis is the well known Chernoff bound.

Theorem 7 (The Chernoff Bound): Let $X = \sum_{i=1}^{n} X_i$ be the sum of n independent random variables, each in $[0, \delta]$. Let $\epsilon \in (0, 1]$, and $\mu > 0$, be fixed. Then,

- If $E[X_i] \leq \mu$ for all i, then $\Pr[X \geq (1+\epsilon)\mu n] < exp[-\epsilon^2 \mu n/(3\delta)]$.
- If $E[X_i] \geq \mu$ for all i, then $\Pr[X \leq (1-\epsilon)\mu n] < exp[-\epsilon^2 \mu n/(2\delta)]$.

We can now state the main result.

Theorem 8: Let $0 \leq p \leq 1$ be fixed. Then,

- If $p < \alpha$ then using only one round of decoding, i.e., only the row code, the decoder successfully decodes any received word almost always.
- If $p > \alpha$ then no matter how many rounds of decoding are used, the decoder fails to decode any received word almost always.

Proof: Assume $p < \alpha$. Choose some fixed $0 < \epsilon < \alpha/p - 1$. Using the Chernoff bound of Theorem 7, any given row contains less than αn errors with probability tending to 1 exponentially fast. Hence, by a simple union bound, the probability of the event that there is some undecodable row in the first round, tends to 0 exponentially fast. Hence, the first round of decoding successfully corrects all errors almost always.

If $p > \alpha$, choose some fixed $0 < \epsilon < 1 - \alpha/p$. Just like the previous case, the probability that any given row or column contain less than αn errors tends to 0 exponentially fast by the Chernoff bound. Hence, given a received word, by a simple union bound, the probability that there is any row or column which is decodable tends to zero exponentially fast. This means, that almost always the decoder fails on all the rows and all the columns. Hence, no matter how many rounds are used, the decoding process fails almost always. ■

V. Conclusion

We analyzed the asymptotic probability of decoding failure of iterative decoders for product codes. Our analysis is limited to the case of hard-decision decoding over the erasure channel. We examined both the case of codes capable of correcting a constant number of errors in each row and column, and the case of codes capable of correcting a constant fraction of the length of each row and column.

In the case of constant error correction, the asymptotic probability shows a threshold behavior. As shown in Table I, when the erasure probability decays faster than the threshold function, we can correctly decode every received word almost always. Conversely, when it decays slower, we almost always fail to decode any received word. When the erasure probability decays just like the threshold function up to a multiplication by a constant, we have an exact expression for the probability of decoder failure. It should be noted, that it is beneficial to invest in more rounds of decoding, and codes which correct more errors, since both $e_T(r,t)$ and $a_T(r,t)$ are increasing functions and $a_T(r,t)$ grows faster than $e_T(r,t)$. This means that higher values of r and t give threshold functions closer to n^{-1}, and higher probability of successfully decoding when the erasure probability is at the threshold.

The other case, of linear error correction capabilities, is perhaps more curious. Again we have a sharp threshold behavior, and in this case, it is constant. However, above this threshold, we almost always have too many errors for each row or column to correct and we fail, no matter how many rounds of decoding we do. Below this threshold, we almost always eliminate all the errors after the first round of decoding, so one round of decoding is enough. In that case, we do not get to use the column code at all, and the redundancy invested in it – is simply redundant. So it appears in that case, that it is better to use just the row code instead of the product code.

Acknowledgment

This work was supported by a research grant from Applied Micro Circuits Corporation, San Diego, CA. The authors would also like to thank Roy Schwartz for some helpful discussions.

References

[1] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*. North-Holland, 1978.

[2] K. A. S. Immink, *Coding techniques for digital recorders*. Prentice-Hall, 1991.

[3] P. G. Farrell, "A survey of array error control codes," *Information Processing*, vol. 3, no. 5, pp. 441–454, 1992.

[4] N. Alon and J. Spencer, *The probabilistic method, second edition*. John Wiley & Sons, Inc., 2000.

[5] S. Janson, "Poisson approximation for large deviations," *Random Structures and Algorithms*, vol. 1, pp. 221–230, 1990.